AF/2134
IAU

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Serial No.:	09/502,478
Filing Date:	2/11/2000
Applicant(s):	Kira Serling Attwood, et al
Entitled:	TECHNIQUE OF DEFENDING AGAINST NETWORK CONNECTION FLOODING ATTACKS
Group Art Unit:	2134
Attorney Docket No.:	RSW9-99-129 (7161-142U)

CERTIFICATE OF MAILING

I hereby certify that the following documents are being deposited with the United Sates Postal Service in an envelope with sufficient postage as first-class mail addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, on June 7, 2005.

- Transmittal for Appeal Brief
- Appeal Brief
- Return receipt postcard

Respectfully submitted,

Peggy Shock

Peggy Shock, Legal Assistant to
Steven M. Greenberg
Registration No. 44,725
Christopher & Weisberg, P.A.
200 East Las Olas Boulevard, Suite 2040
Fort Lauderdale, FL 33301

35619

Docket No.: RSW9-99-129US1 (7161-142U) **PATENT**

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

In re Application of	:	Customer Number: 46320
Kira ATTWOOD, et al.	:	Confirmation Number: 5209
Application No.: 09/502,478	:	Group Art Unit: 2134
Filed: February 11, 2000	:	Examiner: T. Ho

For: TECHNIQUE OF DEFENDING AGAINST NETWORK CONNECTION FLOODING ATTACKS

TRANSMITTAL OF APPEAL BRIEF

Mail Stop Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

Submitted herewith is Appellants' Appeal Brief in support of the Notice of Appeal filed May 16, 2005. Please charge the Appeal Brief fee of $500.00 to Deposit Account 09-0461.

To the extent necessary, a petition for an extension of time under 37 C.F.R. § 1.136 is hereby made. Please charge any shortage in fees due under 37 C.F.R. §§ 1.17, 41.20, and in connection with the filing of this paper, including extension of time fees, to Deposit Account 09-0461, and please credit any excess fees to such deposit account.

Respectfully submitted,

Christopher & Weisberg, P.A.

Steven M. Greenberg
Registration No. 44,725
Christopher & Weisberg, P.A.
200 E. Las Olas Blvd., Suite 2040
Fort Lauderdale, FL 33301
Tel: (954) 828-1488
Facsimile: (954) 828-9122

Date: June 7, 2005

TABLE OF CONTENTS

Page

I. REAL PARTY IN INTEREST 2

II. RELATED APPEALS AND INTERFERENCES 2

III. STATUS OF CLAIMS 2

IV. STATUS OF AMENDMENTS 3

V. SUMMARY OF CLAIMED SUBJECT MATTER 3

VI. ISSUES TO BE REVIEWED ON APPEAL 3

VII. THE ARGUMENT 4

VIII. CLAIMS APPENDIX 12

Docket No.: 7161-142U **PATENT**

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

In re Application of	:	Customer Number: 31292
Kira ATTWOOD, et al.	:	Confirmation Number: 5209
Application No.: 09/502,478	:	Group Art Unit: 2134
Filed: February 11, 2000	:	Examiner: T. Ho

For: TECHNIQUE OF DEFENDING AGAINST NETWORK CONNECTION FLOODING ATTACKS

APPEAL BRIEF

Mail Stop Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

This Appeal Brief is submitted in support of the Notice of Appeal filed May 16, 2005, wherein Appellants appeal from the Examiner's rejection of claims 1-16.

I. REAL PARTY IN INTEREST

This application is assigned to International Business Machines Corporation by assignment recorded on February 11, 2000, at Reel 010606, Frame 0981.

II. RELATED APPEALS AND INTERFERENCES

Appellants are unaware of any related appeals and interferences.

III. STATUS OF CLAIMS

Claims 1-16 are pending and finally rejected in this Application. It is from the final rejection of claims 1-16 that this Appeal is taken.

IV. STATUS OF AMENDMENTS

No amendment to the claims has been filed subsequent to the Final Office Action dated April 15, 2005.

V. SUMMARY OF CLAIMED SUBJECT MATTER

Independent claims 1, 5, 9, and 13 are respectively directed to a method, apparatus, storage media and carrier for preventing a flooding attack on a network server. As stated in the paragraph spanning pages 2 and 3 of the specification, "the consequences of intentional flooding attacks and unintentional overload situations resulting from a burst of connection requests can be mitigated by dropping the traditional notion of attempting to distinguish between legitimate and illegitimate traffic." Rather, in the present invention, "all network traffic is subjected to a policy that attempts to guarantee that legitimate work will be performed and a server will not crash in flooding situations, irrespective of whether the flooding is caused by legitimate or illegitimate traffic." As recited in the claims, in response to a request from a host for a connection to a port number on the server, if the number of connections to the port assigned to the requesting host exceeds a prescribed threshold (see reference numeral 114 in Fig. 1), then the connection is denied. By monitoring the number of connections to a port by a particular requesting host, the claimed invention can reduce flooding regardless on whether the traffic is legitimate or illegitimate.

VI. ISSUES TO BE REVIEWED ON APPEAL

1. Claims 1-16 were rejected under 35 U.S.C. § 102 for anticipation based upon Chebrolu, U.S. Patent No. 6,754,714; and

2. Claims 1, 5, 9, and 13 were rejected under 35 U.S.C. § 102 for anticipation based upon Mutaf.

VII. THE ARGUMENT

THE REJECTION OF CLAIMS 1-16 UNDER 35 U.S.C. § 102 FOR ANTICIPATION BASED UPON CHEBROLU

For convenience of the Honorable Board in addressing the rejections, claims 3, 5, 7, 9, 11, 13, and 15 stand or fall together with independent claim 1. Claims 6, 10, and 14 stand or fall together with dependent claim 2, and claims 8, 12, and 16 stand or fall together with dependent claim 4.

The factual determination of anticipation under 35 U.S.C. § 102 requires the identical disclosure of each element of a claimed invention in a single reference. As part of this analysis, the Examiner must (a) identify the elements of the claims, (b) determine the meaning of the elements in light of the specification and prosecution history, and (c) identify corresponding elements disclosed in the allegedly anticipating reference. That burden has not been discharged. Moreover, the Examiner neither clearly designated the teachings in Chebrolu being relied upon nor clearly explained the pertinence of Chebrolu. In this regard, the Examiner's rejection under 35 U.S.C. § 102 also fails to comply with 37 C.F.R. § 1.104(c).[1]

[1] 37 C.F.R. § 1.104(c) provides:

> In rejecting claims for want of novelty or for obviousness, the examiner must cite the best references at his or her command. When a reference is complex or shows or describes inventions other than that claimed by the applicant, the particular part relied on must be designated as nearly as practicable. The pertinence of each reference, if not apparent, must be clearly explained and each rejected claim specified.

Independent claim 1 recites, in part, the following limitation:

> determining, in response to a request from a host for a connection to a port number on the server, if the number of connections to the port assigned to the host exceeds a prescribed threshold.

In the Final Office Action dated April 15, 2005 (hereinafter the Final Office Action), specifically on page 5, the Examiner recited the above-reproduced limitation word-for-word in the statement of the rejection and merely asserted that this limitation is disclosed within column 2, lines 20-25 of Chebrolu. For ease of reference, column 2, lines 20-25 of Chebrolu is reproduced below:

> For the sake of simplicity in FIG. 1 (and in similarly arranged FIG. 2), a given client is shown connected with a given ISP, but it will be understood that a single client typically may be connected with any one or more of plural ISPs, and that any one or more of plural clients may be connected with a single ISP.

As noted above, the Examiner has failed to identify the elements of claim 1. For example, with regard to the above-reproduced limitation, if the Examiner had identified elements within this limitation, the Examiner would have determined that the elements within this limitation at least include:

(i) a recognition of a particular host connected to a port on the server,
(ii) a determination of the number of connections the particular host has to the port, and
(iii) a comparison of the number of connections the particular host has to the port with a prescribed threshold.

Assuming arguendo that the Examiner identified the above elements and construed a meaning for these elements, the Examiner is also obligated to clearly designate the teachings in Chebrolu being relied upon to teach these elements. That the Examiner did not identify these elements, however, is not surprising since these elements are <u>not</u> identically disclosed by Chebrolu within the citation offered by the Examiner. For example, although Chebrolu discusses a client (i.e., host) connected to an ISP (i.e., server), there is no indication of a recognition of the port to which the client is connected. Furthermore, there is no indication that Chebrolu teaches determining the number of connections the particular host has to the port. Moreover, Chebrolu does not teach comparing the number of connections a particular host has to the port on the server to a prescribed threshold.

Independent claim 1 further recites, in part, the following limitation:

> denying the request for a connect [when the number of connections to the port by a host exceeds a prescribed threshold].

On page 6 of the Final Office Action, the Examiner asserted that this limitation is disclosed within column 1, lines 24-30 of Chebrolu. For ease of reference, column 1, lines 24-34 of Chebrolu is reproduced below:

> If all available channels on a given NAS are allocated among various users, then no new users can obtain access because there is no available channel. Thus, during busy times, many would-be users will be denied access to their desired ISP by the NAS.
>
> A user who requests a secondary channel may use the channel, and may benefit from the increased download bandwidth, only for a short period of time compared to the amount of connect time, i.e. the duration of the session.

The bracketed portion of independent claim 1 reproduced above is the condition that precedes "denying the request for a connect." As noted above, the "number of connections" referred to the claimed invention refers to the number of connections a particular host has with a port on the server. In contrast, the Chebrolu discusses the availability of "channels on a given NAS [that] are allocated among various users." Thus, Chebrolu fails to teach or suggest denying a request for a connect when the number of connections to a port on the sever by a host exceeds a prescribed threshold. Therefore, Appellants respectfully submit that the Examiner has failed to establish that Chebrolu identically discloses the claimed invention, as recited in claim 1, within the meaning of 35 U.S.C. § 102.

Claim 2

Claim 2 recites, in part, the following limitation:

> overriding the denial and allowing the request if a quality of service parameter pertaining to the requesting host permits the override.

On page 6 of the Final Office Action, the Examiner asserted that the following:

> Chebrolu discloses the method of claim 1 in which the deny the request further comprises: Overriding the denial and allowing the request if a quality of service parameter pertaining to the requesting host permits the override, wherein the initial override and denial of the request is overridden (Column 1, lines 45-50), and the request is tended to by allocating to the new user (Column 3, line 20-37) & (Column 4, line 40 - Column 5, line 7), a connection in order to better maintain a quality of service for a greater number of users. (Column 3, lines 15-19).

Similar to claim 1, the Examiner has again failed to identify the elements of claim 2, determine a meaning of the elements, and specifically identify corresponding elements within Chebrolu. Instead, the Examiner jumps from one citation to another throughout Chebrolu to allegedly disclose this straight-forward limitation.

Two of the limitations introduced by claim 2 are that of a "quality of service parameter" and that the quality of service parameter pertains to the requesting host. The Examiner refers to the term "quality of service" and cites column 3, lines 15-19 for support, but a review of this citation (reproduced immediately below) fails to yield a disclosure of a quality of service parameter:

> Apparatus 10 preferably includes a usage table 12, decision logic 14 and allocation logic 16 that cooperate to configure the primary and auxiliary channels for optimum use by the largest possible number of users/clients.

Appellants further note that the "optimum use" referred to in Chebrolu pertains to "the largest possible number of users/clients" and not to a single requesting host, as does the claimed quality of service parameter. The remaining passages cited by the Examiner involve the allocation of channels among users, and particularly to the allocation of channels to users when a primary channel is not available. There is also a discussion of freeing up under-utilized secondary channels when channels are not available. These discussion within Chebrolu, however, fail to teach the claimed limitation recited in claim 2. Therefore, for the reasons stated above, Appellants respectfully submit that the Examiner has failed to establish that Chebrolu identically discloses the claimed invention, as recited in claim 2, within the meaning of 35 U.S.C. § 102.

Claim 4

Claim 4 recites, in part, the following limitation:

> calculating the prescribed threshold by multiplying a percentage P by the number of available connections remaining for the port.

On pages 6 and 7 of the Final Office Action, the Examiner asserted that this limitation is disclosed within column 5, lines 30-37 of Chebrolu. For ease of reference, column 5, lines 30-37 of Chebrolu is reproduced below:

> The invention in this aspect allocates secondary channels along with primary channels only until a prescribed threshold number of allocated secondary channels (or only until a prescribed threshold ratio of allocated secondary channels to allocated primary channels) is reached, after which no further secondary channels are automatically allocated in response to a new user/client request.

As apparent from the plain language of claim 4, the "prescribed threshold" is a value associated with the number of available (i.e., unallocated) connections available for a port. In contrast, the "threshold ratio" disclosed by Chebrolu is between allocated secondary channels and allocated primary channels. Thus, the ratio disclosed by Chebrolu is not comparable to the prescribed threshold recited in claim 4. Therefore, Appellants respectfully submit that the Examiner has failed to establish that Chebrolu identically discloses the claimed invention, as recited in claim 4, within the meaning of 35 U.S.C. § 102.

THE REJECTION OF CLAIMS 1, 5, 9, AND 13 UNDER 35 U.S.C. § 102 FOR ANTICIPATION BASED UPON MUTAF

For convenience of the Honorable Board in addressing the rejections, claims 5, 9, and 13 stand or fall together with independent claim 1.

On page 7 of the Final Office Action, the Examiner merely reproduced, word-for-word, the language of claim 1 and asserted that these features are disclosed within page 6, Section 5 entitled "Detection Method" of Mutaf. For ease of reference, Section 5 of Mutaf is reproduced below:

> **5 Detection Method**
> The detection method that we propose is based on the intensity measures of SYN segments. At time of writing there exists at least one reference which mentions such a possibility[10].
> The parameters that can be associated with the SYN flooding attack are:
>
> ?? *T*: SYN-RECEIVED state timeout in seconds (usually 75).
> ?? *L*: Per-port backlog queue length.
> ?? *A*: Number of received SYN segments per second by a given TCP port.
>
> We call here *A*, as the intensity of SYN segments.
> In order to succeed in a SYN-flooding attack, the minimum number of SYN segments that an attacker must send in *T* seconds is *L*. Thus, the average intensity of SYN segments in *L* seconds must be *L* / *T*. However this is a minimum value and the higher the chosen rate, the more effective the attack will be. We note that, this situation is of considerable advantage in the detection of an attack. An additional parameter needed for our detection method is:
>
> ?? *Ac*: the maximum acceptable (critical) *A* value.
>
> Then, our network monitor computes *A* for each second and for each port of ephesus, and whenever it observes the condition *A* > *Ac* satisfied, it considers the situation as an attack and acts accordingly.

Similar to the rejection based upon Chebrolu, the Examiner has again failed to identify the elements of claim 1, determine a meaning of the elements, and specifically identify corresponding elements within Mutaf.

Notwithstanding the Examiner's failure to identify specific elements within Mutaf that allegedly correspond to elements of the claimed invention, Appellants have reviewed Mutaf and respectfully submit that Mutaf fails to identically disclose the claimed invention. For example, Mutaf fails to teaching recognizing a port to which the client is connected and determining the number of connections the particular host has to the port. Moreover, Mutaf does not teach comparing the number of connections the particular host has to the port on the server to a prescribed threshold. Therefore, Appellants respectfully submit that the Examiner has failed to establish that Mutaf identically discloses the claimed invention, as recited in claim 1, within the meaning of 35 U.S.C. § 102.

Conclusion

Based upon the foregoing, Appellants respectfully submit that the Examiner's rejections under 35 U.S.C. § 102 are not factually or legally viable. Appellants, therefore, respectfully solicit the Honorable Board to reverse the Examiner's rejections under 35 U.S.C. § 102.

To the extent necessary, a petition for an extension of time under 37 C.F.R. § 1.136 is hereby made. Please charge any shortage in fees due under 37 C.F.R. §§ 1.17, 41.20, and in connection with the filing of this paper, including extension of time fees, to Deposit Account 09-0461 and please credit any excess fees to such deposit account.

Respectfully submitted,

Christopher & Weisberg, P.A.

Steven M. Greenberg
Registration No. 44,725
Christopher & Weisberg, P.A.
200 E. Las Olas Blvd., Suite 2040
Fort Lauderdale, FL 33301
Tel: (954) 828-1488
Facsimile: (954) 828-9122

Date: June 7, 2005

VIII. CLAIMS APPENDIX

1. A method of preventing a flooding attack on a network server in which a large number of requests are received for connection to a port number on the server, comprising:

determining, in response to a request from a host for a connection to a port number on the server, if the number of connections to the port assigned to the host exceeds a prescribed threshold, and, if so, denying the request for a connection.

2. The method of claim 1 in which denying the request further comprises:

overriding the denial and allowing the request if a quality of service parameter pertaining to the requesting host permits the override.

3. The method of claim 2 wherein a connection request is denied in any event if the number of available connections to the port are less than a constrained threshold.

4. The method of claim 1or claim 2 or claim 3 further comprising:

calculating the prescribed threshold by multiplying a percentage P by the number of available connections remaining for the port.

5. Apparatus for preventing a flooding attack on a network server in which a large number of requests are received for connection to a port number on the server, comprising:

means for determining, in response to a request from a host for a connection to a port number on the server, if the number of connections to the port assigned to the host exceeds a prescribed threshold, and

means responsive to the determining means for denying the request for a connection.

6. The apparatus of claim 5 in which means for denying further comprises:

means responsive to a quality of service parameter pertaining to the requesting host for overriding a request denial and allowing the request.

7. The apparatus of claim 6 further comprising:

means for denying a connection request in any event if the number of available connections to the port are less than a constrained threshold.

8. The apparatus of claim 5 or claim 6 or claim 7 further comprising:

means for calculating the prescribed threshold by multiplying a percentage P by the number of available connections remaining for the port.

9. A storage media containing program code segments for preventing a flooding attack on a network server in which a large number of requests are received for connection to a port number on the server, comprising:

a first code segment activated in response to a request from a host for a connection to a port number on the server for determining if the number of connections to the port assigned to the host exceeds a prescribed threshold, and

a second code segment responsive to the first code segment for denying the request for a connection.

10. The media of claim 9 in which the second code segment further comprises:

a third code segment for overriding the denial and allowing the request if a quality of service parameter pertaining to the requesting host permits the override.

11. The media of claim 10 further comprising a fourth code segment for denying a connection request in any event if the number of available connections to the port are less than a constrained threshold.

12. The media of claim 9 or claim 10 or claim 11 further comprising:

a fifth code segment for calculating the prescribed threshold by multiplying a percentage P by the number of available connections remaining for the port.

13. A carrier wave containing program code segments for preventing a flooding attack on a network server in which a large number of requests are received for connection to a port number on the server, comprising:

a first code segment activated in response to a request from a host for a connection to a port number on the server for determining if the number of connections to the port assigned to the host exceeds a prescribed threshold, and

a second code segment responsive to the first code segment for denying the request for a connection.

14. The carrier wave of claim 13 in which the second code segment further comprises:

a third code segment for overriding the denial and allowing the request if a quality of service parameter pertaining to the requesting host permits the override.

15. The carrier wave of claim 14 further comprising a fourth code segment for denying a connection request in any event if the number of available connections to the port are less than a constrained threshold.

16. The carrier wave of claim 13 or claim 14 or claim 15 further comprising:

a fifth code segment for calculating the prescribed threshold by multiplying a percentage P by the number of available connections remaining for the port.